Access Control

Visit: www.pgitl.com

Access Control

User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks. Adhering to these simple rules will help protect a system's sensitive data as it will reduce the chance a user will either willingly or unwillingly gain unintended access to sensitive systems.

Access Control

Are user account requests subject to proper justification, provisioning and an approvals process, and assigned to named individuals?

Access Control

Are users required to authenticate with a unique username and strong password before being granted access to computers and applications?

Access Control

Are accounts removed or disabled when no longer required?

Access Control

Are elevated or special access privileges, such as system administrative accounts, restricted to a limited number if authorised individuals?

Access Control

Are special access privileges documented and review regularly (e.g. quarterly)?

Access Control

Are all administrative accounts only permitted to perform administrator activity, with no Internet or external email permissions?

Access Control

Does your password policy enforce changing administrator passwords at least every 60 days to a complex password?

Access Control - CE Overview

- Role Based Access Control
- Least Privilege
- Regular Review and Audit
- Special Access Privileges
- Joiners, Movers and Leavers

RBAC’s

- Method of regulating access to computer systems or networks based on the roles of the individual users.
  - Role Assignment: a subject can exercise permission if the subject has been assigned a role
  - Role Authorisation: a subject can only perform a role if they’ve been authorised
  - Permission Authorisation: a subject can only exercise a permission if the permission is authorised for the subject role.

Least Privilege

- Info Sec principle where a ‘module’ – program, process or user, must only be able to access information and resources which are only essential for performing its purpose.
- By default the module should only be assigned the least privilege to perform its function. All privilege escalations should be justified, reviewed, documented and authorised.

Other Access Control Models

- Bell – LaPadula: access control rules, uses security label on objects and clearances for subjects. ‘No read up, no write down’
- Biba: data integrity model: ‘No read down, no write up’. User can only create content at or below their own level.